Security Profiles

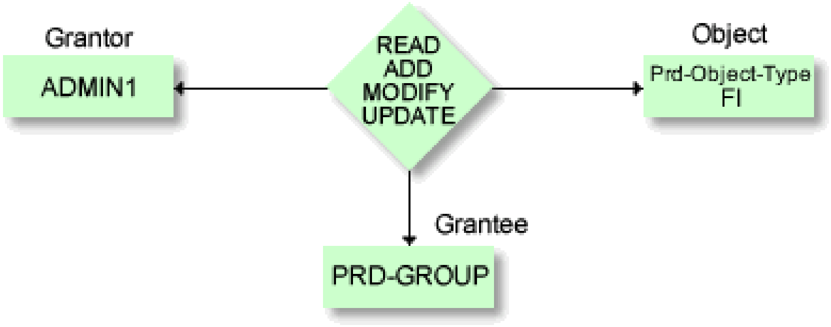
This section covers the following topics:

- General Information
- Defining Access Rights

General Information

The main task of a security administrator consists of granting users access to objects.

This access is defined in Natural Security by means of a complex relationship.



In this example, the security administrator with the user ID ADMIN1 (Grantor) grants the group PRD-GROUP (Grantee) access to NSC external object type FI.

Access can be granted as follows:

- **Natural Security**
  With Natural Security functions you can administer access rights for Predict objects, object types and functions. See also **Natural Security Administration documentation**.
- **Special Function Mass Grant**
  Use the special function Mass to generate security definitions in Natural Security from data in Predict. Only applicable to objects.

Defining Access Rights

What can be Protected?

With security definitons in Natural Security you can protect the following:

- Documentation objects
- Special objects (for example Retrieval Models and Association Types)
- External object types
- Predict functions
- XRef data

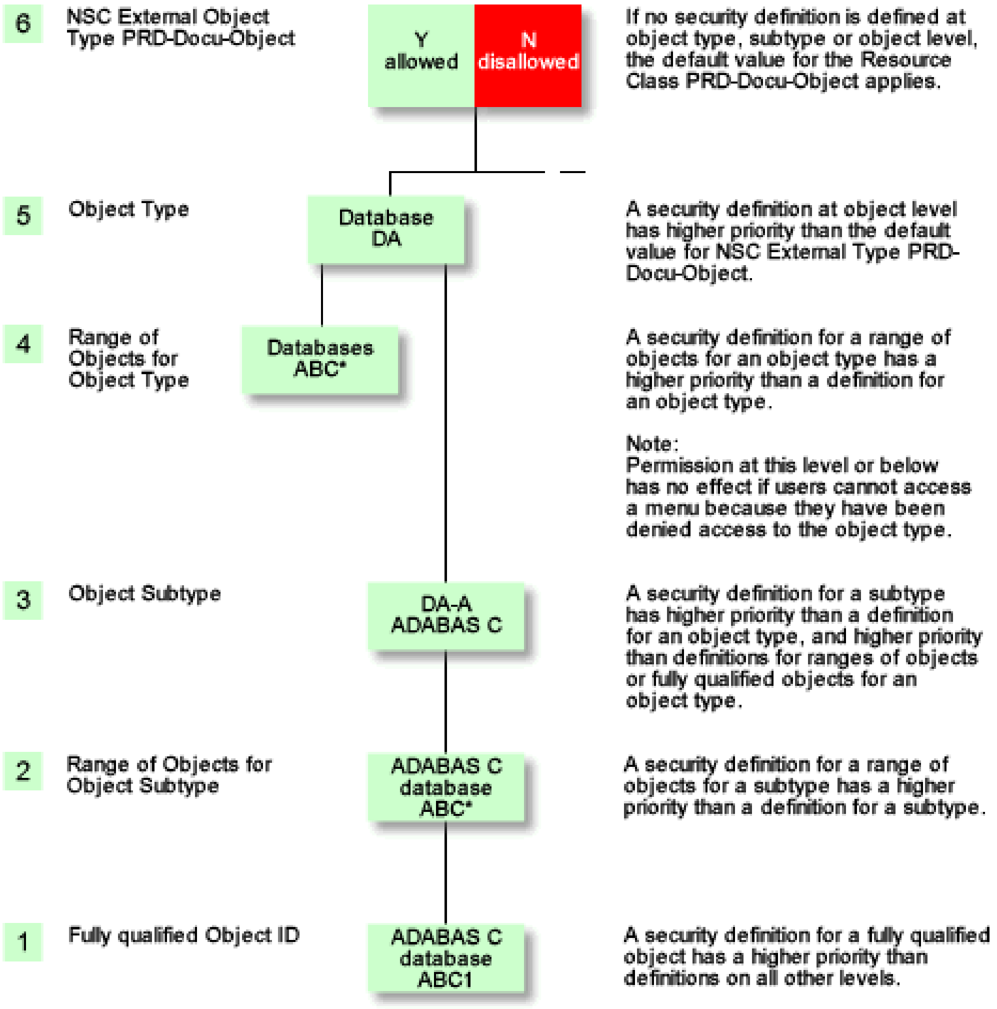
See complete list in Predict Security using Natural Security.

Two Levels of Definitions in Natural Security

There are two levels of security definitions Natural Security:

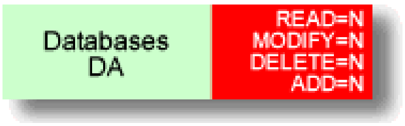
- Each object in Natural Security has a **default** definition. This value is taken when no specific definition for a user or group exists.
- Each object in Natural Security can have a link to a user or group. This link contains a specific security definition for an individual user or a group.

Hierarchy of Security Definitions


6
NSC External Object Type PRD-Docu-Object
Y allowed
N disallowed
If no security definition is defined at object type, subtype or object level, the default value for the Resource Class PRD-Docu-Object applies.
5
Object Type
Database DA
A security definition at object level has higher priority than the default value for NSC External Type PRD-Docu-Object.
4
Range of Objects for Object Type
Databases ABC*
A security definition for a range of objects for an object type has a higher priority than a definition for an object type.
Note:
Permission at this level or below has no effect if users cannot access a menu because they have been denied access to the object type.
3
Object Subtype
DA-A ADABAS C
A security definition for a subtype has higher priority than a definition for an object type, and higher priority than definitions for ranges of objects or fully qualified objects for an object type.
2
Range of Objects for Object Subtype
ADABAS C database ABC*
A security definition for a range of objects for a subtype has a higher priority than a definition for a subtype.
1
Fully qualified Object ID
ADABAS C database ABC1
A security definition for a fully qualified object has a higher priority than definitions on all other levels.

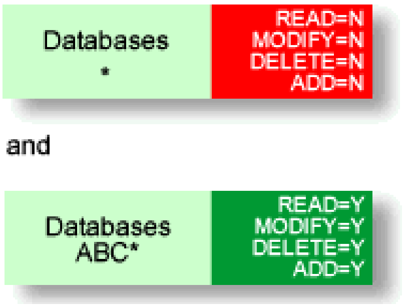
Object and Object Type Level

If you disallow an object type, this object type does not appear in a Predict main menu. This means you cannot process any object of this type. Example:



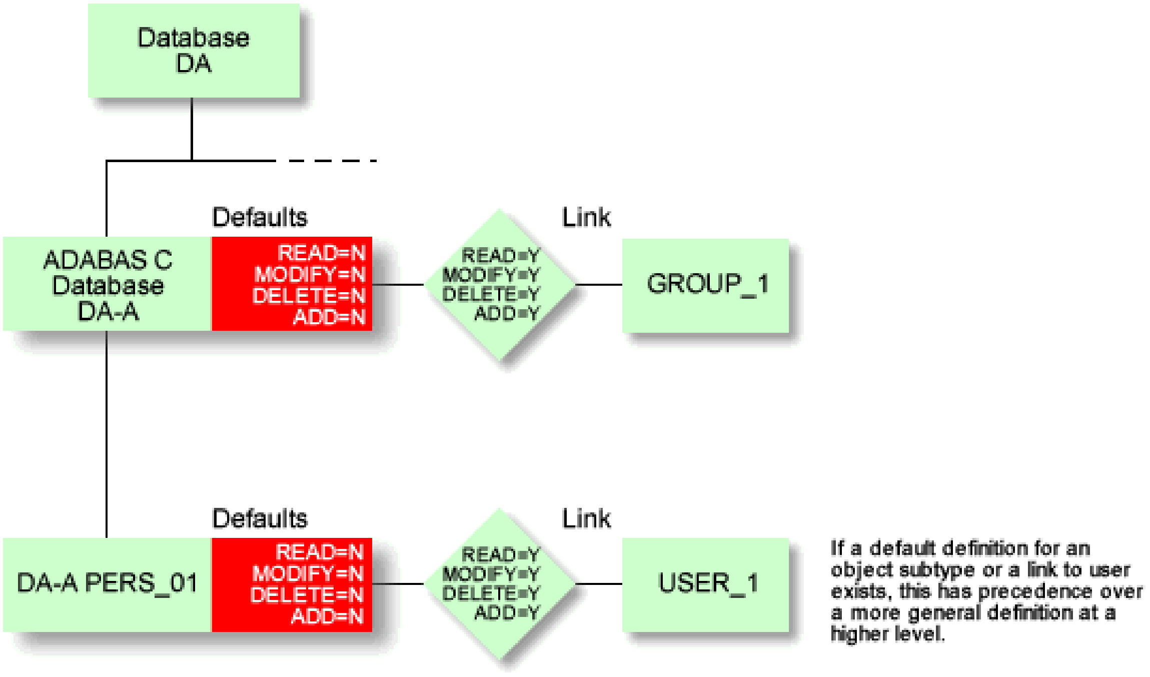
Granting permission for subtypes or for individual objects has no effect, because the user is not able to call the respective menu, for example Maintain Database.

If you wish to prevent access to most databases, for example, but permit access to individual databases, create the following object-level definitions:



In the example above, the user can access only databases which are prefixed with ABC.

Default Definitions and Links to Users



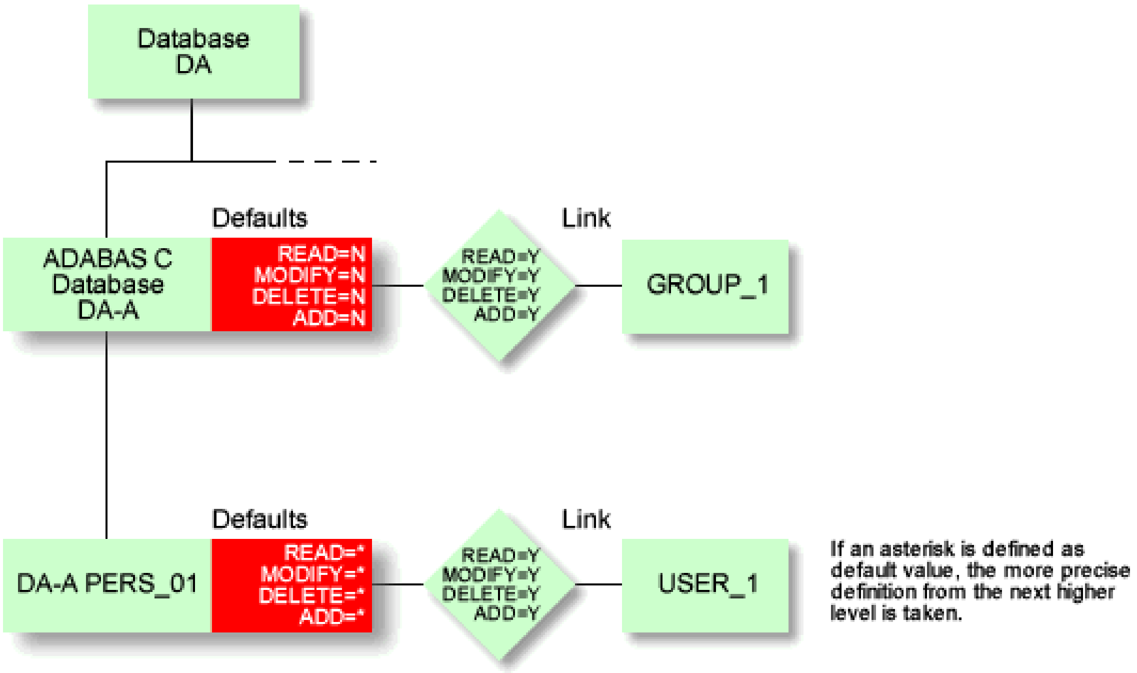
If a default definition for an object subtype or a link to user exists, this has precedence over a more general definition at a higher level.

In this example, members of GROUP_1 have access to Adabas C databases, but do not have access to database object PERS_01. The only user with access to PERS_01 is USER_1.

Recommendation

Because a default definition for an object applies to all users and groups, it can make sense to specify an asterisk as default value.

Default Definitions and Links to Users - with Inheritance



If an asterisk is defined as default value, the more precise definition from the next higher level is taken.

In this example, members of GROUP_1 have access to Adabas C databases, and also access to database object PERS_01.

Sample Security Definitions

Example 1

In this example, all users may read files of type Adabas C, but only members of group DBA-GROUP may modify them.

Object Type	Object	Link to User	READ	MODIFY	DELETE	ADD
FI-A	-	default	Y	N	N	N
FI-A	-	DBA-GROUP	Y	Y	Y	Y

Example 2

In this example, USER1 can only maintain files that start with his user ID. All other users can maintain files starting with their user ID, but not those with user ID USER1.

Object Type Definition

Object Type	Object	Link to User	READ	MODIFY	DELETE	ADD
FI	-	default	Y	Y	Y	Y

Object Definition

Object Type	Object	Link to User	READ	MODIFY	DELETE	ADD
FI	*(=all)	default	N	N	N	N
FI	USER1*	default	*	*	*	*
FI	USER1*	USER1	Y	Y	Y	Y
FI	USER2*	default	*	*	*	*
FI	USER2*	USER2	Y	Y	Y	Y

Example 3

In this example, User1 can maintain only the following files:

- Files of any type that start with his user ID
- Files of type A that start with ABC

He cannot modify

- Files of type V, even those which start with his user ID.

Object Type Definition

Object Type	Object	Link to User	READ	MODIFY	DELETE	ADD
FI	-	default	Y	N	N	N
FI	-	USER1	Y	Y	Y	Y
FI-V	-	default	*	*	*	*
FI-V	-	USER1	Y	N	N	N

Object Definitions

Object type	Object	Link to User	READ	MODIFY	DELETE	ADD
FI	* (=all)	default	*	*	*	*
FI	*	USER1	N	N	N	N
FI-A	ABC*	default	*	*	*	*
FI-A	ABC*	USER1	Y	Y	Y	Y
FI	USER1*	default	*	*	*	*
FI	USER1*	USER1	Y	Y	Y	Y

Areas of Predict that are not protected

Profile

A user can read and use the profile of another user. It is not possible to modify the profile of another user, and it is therefore not necessary to protect profiles separately with Predict Security.

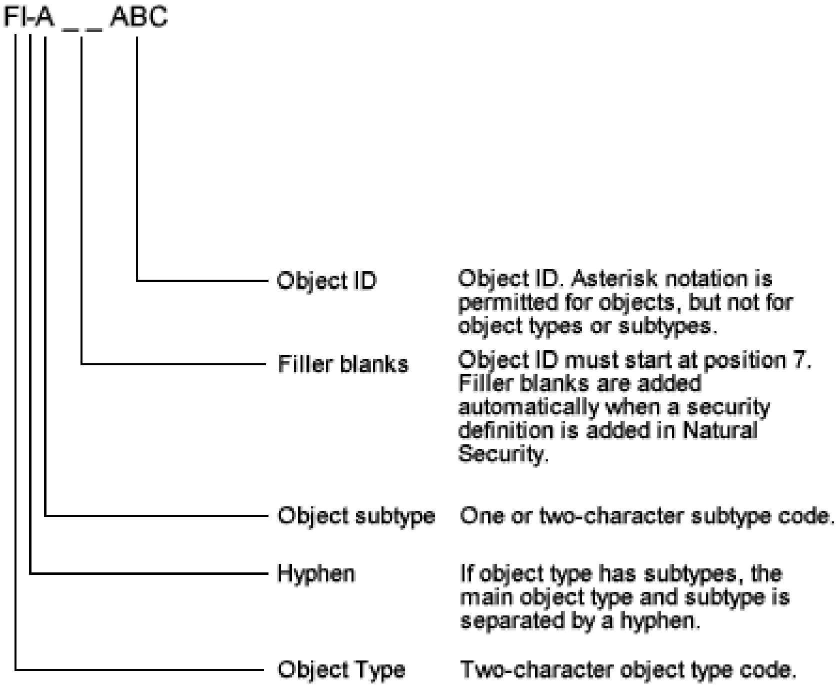
What is new, Help system

No Security checks are performed for these items in the Function Main Menu.

Checks Performed when Adding Security Definitions

The following checks are performed when security definitions are added to ensure that the user is allowed to read the data he wishes to maintain.

- User must have READ access if ADD, MODIFY or DELETE access is granted.
- READ access cannot be denied if the user already has ADD, MODIFY or DELETE access.
- Special syntax must be used when adding a definition for a Predict object. See diagram below.


FI-A _ _ ABC
Object ID
Object ID. Asterisk notation is permitted for objects, but not for object types or subtypes.
Filler blanks
Object ID must start at position 7. Filler blanks are added automatically when a security definition is added in Natural Security.
Object subtype
One or two-character subtype code.
Hyphen
If object type has subtypes, the main object type and subtype is separated by a hyphen.
Object Type
Two-character object type code.

Example: if you enter object FI(blank)ABC*, the name is changed to the correct syntax automatically: FI(blank)(blank)ABC*.

Tips and Tricks

Deny Globally, Grant Locally

In Example 1 below, individual subtypes or functions are allowed and at the same time all others disallowed.

Example 1

In this example the user is granted EXECUTE access to Special Function Recover but is not allowed to access any other Special Functions.

Function	EXECUTE	Note
SPECIAL-*	N	All Special Functions are disallowed.
SPECIAL-RECOVER	Y	Special Function Recover is allowed. This specific definition has priority over the general definition.

> **Note:**
> If you disallow SPECIAL* (without hyphen), the Special Function Menu is also disallowed. This means that all special functions are disallowed.

Granting Access to a Range of Files

In Example 2, the user may only read files with a certain prefix.

Example 2

Object Type	READ	Note
FI	Y	This definition is not required if the default value = Y..

Object	READ	Note
FI *	N	READ access to all files is disallowed.
FI ABC*	Y	READ access is allowed for files starting with ABC. This definition has a higher priority than the general definition at the same level and does not contradict the definition at the higher level.

Restrict Function to a specific Group

Example 3

In Example 3, only members of group SEC-DBA are allowed to execute the Special Function Protection.

	EXECUTE		
Function	Default	for Group SEC-DBA	Note
SPECIAL-PROTECTION	N	Y	Security definitions for individual groups always have a higher priority than default definitions.

Definitions at Subtype Level have Priority over Definitions for the Main Object Type

Example 4

Object Type	READ	Note
FI	Y	
FI-A	N	User may not read any files of type Adabas.

Object	READ	Note
FI TEST*	Y	User may read files that start with TEST, but not those of type Adabas.